Lecture 3
Trust and Networks

CS3690 Network Security

Summer Quarter, 2000

C. Irvine

Objectives

- Consider Network Abstraction
- Examine Security Service Placement
- Consider Selected Network Components

Secure Network Abstraction

- There are users and information
- Access to information is provided to users according to a security policy
- Identification of the users must be properly maintained so that the security policy is correctly enforced.
  - user name attribute
  - user security level attribute
- For accountability purposes, an audit trail may also be maintained
- Each user can be thought to be physically accessing a single component on the network. This is the user's local component
- Other components are accessed transitively via the local component.
  These are remote components.

Summer Quarter, 2000 C. Irvine; NPS CISR 3

Subjects and Objects

- A fundamental technical notion is that of subjects and objects.
  - objects are passive repositories storing information
    - Where is information stored?
    - Is it information if it isn't captured?
  - subjects are active entities which will attempt access to objects
    - Where do subjects execute?
- The secure system must provide the following functions
  - User identification and authentication
  - Transitive association of users' identity with system subjects
  - Access decisions based upon user attributes
  - Audit collection

Summer Quarter, 2000 C. Irvine; NPS CISR 4

Network Components

- Servers
- Communications Medium
- Clients

Relationship Between Network Components

- Suppose the user is logged into a local component and attempts to access services from a remote component.
  - ★ The local component can be considered to be a client
    - In the client there will be a subject that acts on behalf of the user.
  - ★ The remote component is a server
    - In the remote component there will be a subject that acts on behalf of the user
- Using a protocol the client subject will request services from the server. The protocol could initially activate a subject on the user's behalf.

Protocols

- We observe that the layers of the ISO stack will have individual protocols. How can the protocols at the ISO stack layers can be made to work together to provide a coherent mechanism for security policy enforcement?
- Questions:
  - Do clients request services from servers and then wait for the server to reply?
  - Do servers make requests of clients that are not initiated by the clients?
  - Can the servers notify clients of events?
  - Does the server depend upon the client in order to respond?
  - For each service, will there be a specific service protocol?
  - Can the roles of Clients and Servers be reversed?

Protocols in Action - Local Start Up

1. local component identifies user (T)
2. local component creates an application subject with user-related attributes (T)
3. local application subject executes and requests information from local objects
4. local system-level subject makes access checks and, based upon these, returns information contained in object (T)
5. local application subject wishes access to remote information
6. local application subject requests connection to remote host. Request for connection is mediated within the local system. (T)
7. local system-level subject initiates connection request service protocol identified with user. User attributes are part of the protocol. (T)

How many subjects have worked on the protocol so far?

Protocols in Action - Remote Response

8. remote system mediates request for connection. (T)
9. remote server system level subject receives request and creates a server subject associated with the user's ID. (T) This subject is performing a particular role on the part of the user, e.g. engineer, marketing, finance
10. remote user-role subject requests access to remote information.
11. request is mediated by policy enforcement mechanism in remote system. (T)
12. reply is returned via a request to the system-level server subject handling the connection to the client. (Note that the ability to reply is also mediated, but this may have been accomplished as part of the request for connection. That is, the connection is bi-directional). (T)
13. client application subject receives the information.
14. audit information may be obtained for all, none, or some subset of these steps. (T)

Summer Quarter, 2000 C. Irvine; NPS CISR 9

Security Considerations

- Each component maintained its own security policy and mediated access to the objects it controlled.
- Each component made security decisions regarding its communications to remote components.
  - ★ Do I wish to establish a connection in which I will write to that component?
    - For mandatory security the question can be put in terms of the simple security property for confidentiality. I will only write to entities that are of equivalent or higher secrecy than my subject.
  - ★ Do I wish to establish a connection in which I will read from that component?
    - For mandatory security the question can be put in terms of the simple security property for integrity. I will read information that is only of equivalent or higher integrity than my subject.

Summer Quarter, 2000 C. Irvine; NPS CISR 10

Connection -- A Multidimensional Problem

- Ability to establish a connect is multidimensional and, in fact, the server connection protocol subjects acting on behalf of many user applications may have a range of secrecy and integrity levels.
- The network security architecture reflects a policy that may be monolithic across the components of a particular organization, but must also permit that organization to communicate with the external world.

Network Security Invariants

1. All protocols in the enterprise network security architecture will be defined.
2. All components of the network will be uniquely identified
3. All subjects will be identified via trusted mechanisms prior to access to the network
4. Authentication data shall be protected from object reuse.
5. All active entities in the network (subjects) will be uniquely identified
6. Network services will only be provided by trusted software
7. Application (untrusted) subjects will communicate with each other using the underlying trusted components
8. Local access to objects shall be mediated by local policy.
9. Access to objects across the network shall be mediated according to policy (DAC and/or MAC)

Network Taxonomy

- Network
  - A collection of interconnected functional units which include both hardware and software that provides communications services between endpoints attached to the network
- Internet
  - A collection of networks connected together by bridges and/or gateways. Also called an Internetwork.
- Subnet
  - A network that is a component of an internet. Also called a subnetwork. It is what a user would call a single network.

Summer Quarter, 2000 C. Irvine; NPS CISR 13

System Terminology

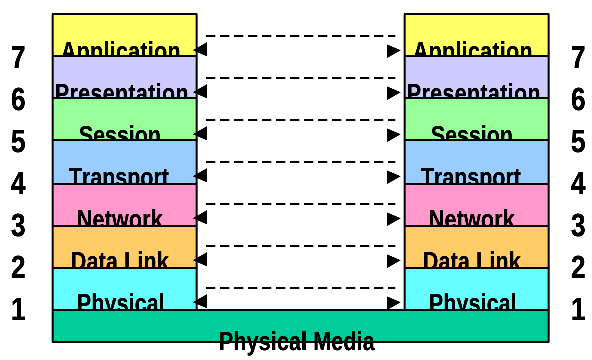
- End System (ES)
  - A host system in which the end-user application of a communication service executes
- Intermediate System (IS)
  - A host system that performs relay operations in support of communications services between end systems.Note that a single host can play the role of both an end system and an intermediate system.
    - Bridge - an intermediate system used to connect two LANs using identical LAN protocols
    - Router - an IS used to connect to possibly dissimilar networks
- Network Medium
  - The physical carrier of information

Summer Quarter, 2000 C. Irvine; NPS CISR 14

Models of Networks

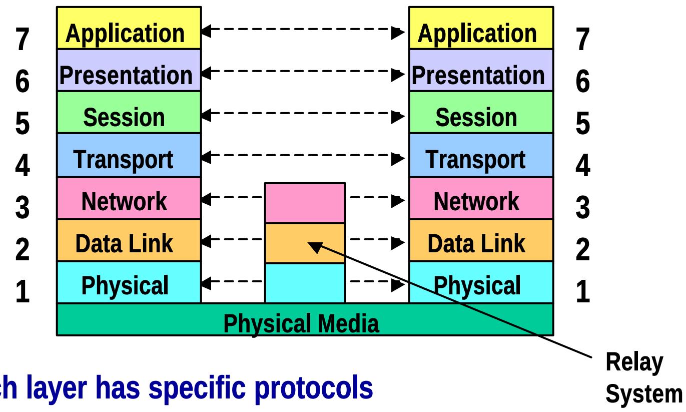
- Systems modeled in terms of layers. Provides
  - Provides common framework for discussing the functions provided by the system.
  - Real systems do not precisely follow Model
    - Combine layers.
- Two principle models for network communications protocols
  - OSI
  - TCP/IP
- The idea is that a system is built out of some number of layers and that at layer N there is a protocol which defines how N-entities communicate with each other
  - Format or syntax
  - Semantics or meaning
- The N-layer will present a service interface to higher layers (the N:+1) layer and will utilize the services of the N-1 layer.We say that when a message is sent using the N-layer protocol that it is an N-protocol data unit (PDU), e.g. an Application PDU.
- Important: notice lack of *circular dependencies.*

Layered Network Architectures



- Lowest layers - physical network
- Middle layers - connections and messages
- Upper Layers - interfaces to users and support applications

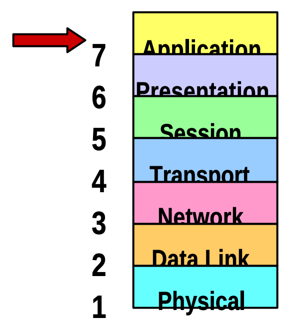
Network Layer Functions



- Each layer has specific protocols
- Each Layer supports specific security services
- Intermediate elements - a variety of technolgies

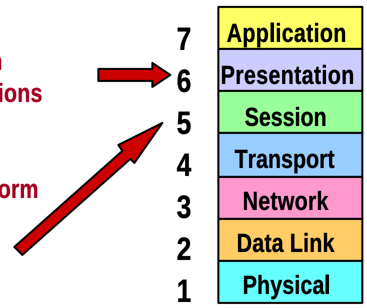
Application Layer (7)

- Protocols and communications standards apply to particular applications or families of applications
- Network Services
  - file transfer
  - directory services
- Network Utilities
  - electronic mail
  - EDI services
  - voice messaging



Presentation Layer (7) & Session Layer (6)

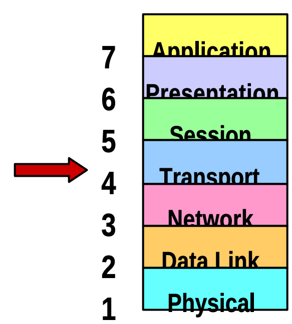
- **Presentation Layer (6)**
  - protocols to represent information to the application layer entities for communications purposes. These are host specific and convert the information into a canonical form for the applications
- **Session Layer (5)**
  - supports synchronization for data exchange management (often absent)



Summer Quarter, 2000 C. Irvine; NPS CISR 19

Transport Layer (4)

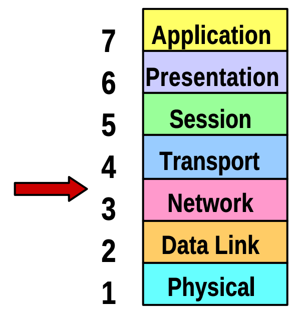
- Provides reliability and cost-effective data transfer
- Provides communication reliability by sequencing packets.
- Eerror detection and recovery services
  - packet numbers on outgoing packets
  - holding incoming packets so that they are delivered in the correct order
  - retransmission of lost packets
  - multiplexing of transport connections on one network connection
- Several classes of service are possible. With the highest a connection-oriented transport service can be presented to higher layers while the transport layer is riding on a connectionless network layer



Summer Quarter, 2000 C. Irvine; NPS CISR 20

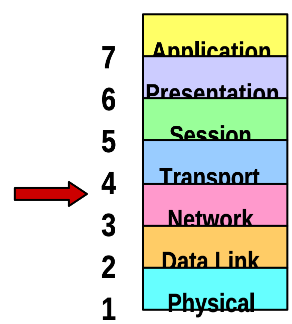
Network Layer (3)

- Hides routing and relay considerations from upper layers. Routers found here. Upper layers do not see how data links are used.
- Paths are computed across links and packet switches.
- Responsible for forwarding packets across multiple links to move the information from the source to the destination. Thus it provides indirect communication between network endpoints located in hosts.
- Connection-oriented or connectionless
- Includes an internetworking sublayer



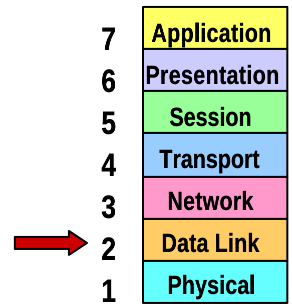
Network Layer (3) and Subnets

- Hides possible multiple subnetworks from higher level layers.
  - subnets may be built using quite different interconnection and media technologies
  - Highly complex layer.
- Some of the subnet technologies supported by
- Network Layer Protocols include:
  - Local Area Networks
  - Packet Switched Data Networks (X.25
  - Circuit Switched Networks
  - Point-to-Point Networks
  - Integrated Services Digital Networks
  - Public Switched Telephone Networks



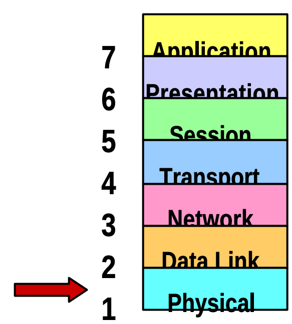
Data Link Layer (2)

- Point-to-point data transfer.
  - Bridges are associated with this layer.
  - Establishes, maintains, and releases point-to-point connections.
- Detection/correction for errors that may occur in the physical layer.
  - Several different Ethernet frame formats that protocols in this layer may need to support.
- Two important protocols at this layer:
  - MAC (Medium Access Control) which provides an address space comprised of an IEEE assigned portion (3 bytes) and a NIC vendor assigned portion (3 bytes)
  - LLC (Logical Link Control) for addressing multiple MAC addresses and flow control



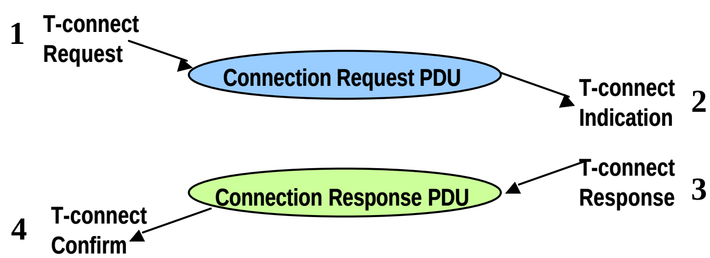
Physical Layer (1)

- Mechanical, functional, electrical, procedural mechanisms for physical connections.
- Connections are activated, deactivated, and maintained.
- Layer would describe repeaters.
- For a LAN these include, for example, twisted pair Ethernet (10BaseT)



Protocols

- At each layer, facilities created from service primitives.
  - small atomic actions
  - usually send message to recipient in the form of a protocol data unit (PDU).
- Example: transport facility to create a transport connection.
  - 2 service primitives at each end and 2 PDUs sent across network.



- This is an example of a confirmed service. What would an unconfirmed service look like?

Protocol types

- Two types of protocols:
  - Connection-oriented: establish, transfer, release. During transfer a datastream is passed on behalf of higher protocol layers.
  - Connectionless: single data units are sent. There is no acknowledgement of receipt. In fact, data units may take physically different routes across the network.

TCP/IP Model

TCP/IP Notions

- Three principle entities
  - Processes
  - Hosts
  - Networks
- Processes execute on hosts and communicate with each other across the networks to which hosts are connected

Application Protocol Standards

- FTP - file transfer
- HTTP - web
- SSL - secure sockets layer
- SMTP - email
- SNMP - network management
- TELNET - remote login
- DNS - Directory Name Service

Lower Layer Protocols

- Transport and Network Layer Protocols
  - TCP
    - connection-oriented
    - reliable communication path (virtual circuit)
  - UDP
    - connectionless transport protocol
- Internet Protocol
  - IP
    - connectionless protocol

Placement of Security Services

- Application level
- Application-dependent security protocol elements required when
  - ★ security services are application specific and may be built into the semantics of a particular application protocol.
    - Example: protection of a PIN in a financial transaction.
  - ★ security services traverse application relays
    - e-mail is an example: we need to protect the content of the message, but other aspects of the message such as address fields must be visible to the relay system.

Summer Quarter, 2000 C. Irvine; NPS CISR 31

End System Service Placement

- End-system to end-system protocol elements required when
  - ★ Underlying communications networks are untrusted, although end systems are trusted
  - ★ Required by an authority
    - application security services don't matter
  - ★ Requirements relating to the connection.
    - Example: confidentiality for all communications on a particular connection.
- Why often better than application-level solution?
    - applications can be "security independent"
    - performance may be enhanced
    - administration of security services may be more centralized
    - protocol headers for higher layers are protected.

Summer Quarter, 2000 C. Irvine; NPS CISR 32

End-to-End Choices

- There are layering choices for end-system security
- Transport Layer
  - ★ different grades of protection can be provided to different transport connections
  - ★ protection goes directly to the end system. A number of vulnerabilities are avoided·
- Network Layer
  - ★ the same solution may be provided at the end-system as well as the subnetwork components.
  - ★ special security devices may be inserted transparently
  - ★ any upper layer architecture may be supported.

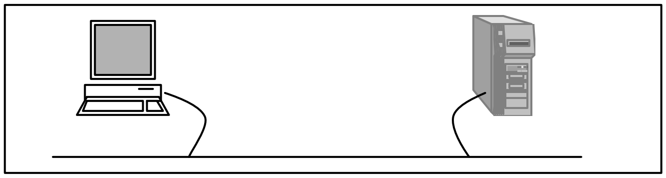
Summer Quarter, 2000 C. Irvine; NPS CISR 33

Lower Layer Security Placement

- There are layering choices for end-system security
- Transport Layer
  - ★ different grades of protection can be provided to different transport connections
  - ★ protection goes directly to the end system. A number of vulnerabilities are avoided
- Network Layer
  - ★ the same solution may be provided at the end-system as well as the subnetwork components
  - ★ special security devices may be inserted transparently- any upper layer architecture may be supported.

Summer Quarter, 2000 C. Irvine; NPS CISR 34

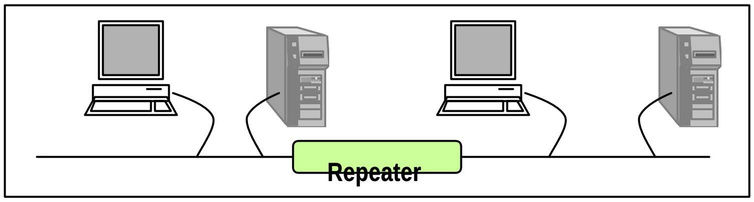
Physical Network Topologies: Simple LAN



- How does the workstation communicate with the server?
- By sending a packet directly. The addressing for the source and destination are determined by the link-layer addressing and are unambiguous

Summer Quarter, 2000 C. Irvine; NPS CISR 35

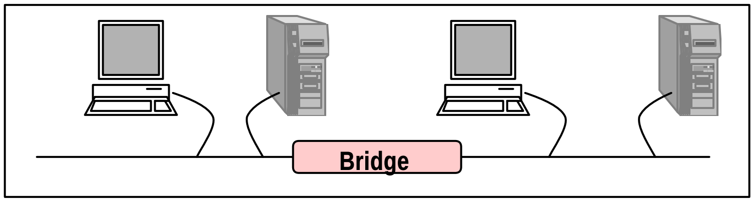
Repeater Connected LAN



- The element in between the LANs is a repeater. It could be a hub. There is no additional security service provided by this element. This means that we can view the repeater-connected LAN as if it were a simple LAN.

Summer Quarter, 2000 C. Irvine; NPS CISR 36

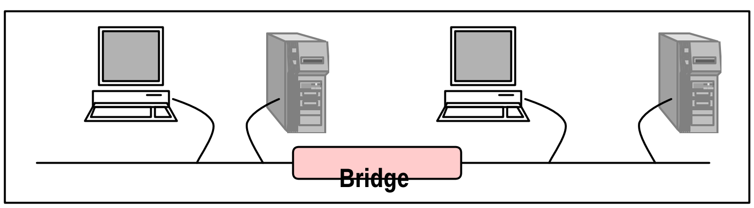
Bridge Connected LAN



- Bridge copies packets from one LAN to another.
  - ★ Determines packets to copy using Link Layer addresses.
  - ★ Both LANs must use the same link layer protocol. The bridge understands this protocol.
  - ★ Does Bridge Modify Link Layer Addresses?
  - ★ Does Bridge Perform Security Functions
  - ★ Logically is this the “same” LAN?

Summer Quarter, 2000 C. Irvine; NPS CISR 37

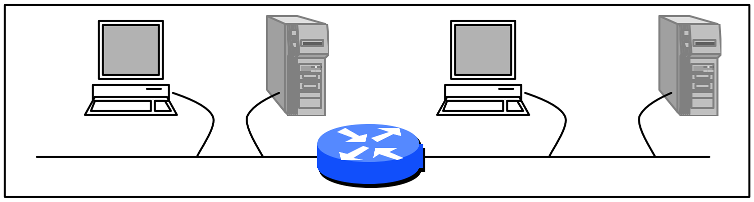
Bridge Connected LAN



- From the logical point of view, can a LAN composed using both bridges and repeaters be the same LAN?
- Answer will depend upon the LAN topology. If we construct a LAN such that packets must be replicated, then the composite LAN is different.
- Thus, in order to call it logically equivalent to a simple LAN, we must place a restriction that disallows configurations that would result in packet replication.

Summer Quarter, 2000 C. Irvine; NPS CISR 38

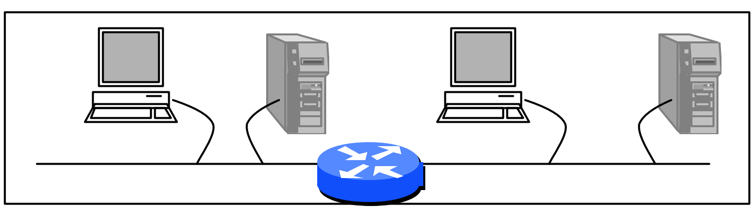
Router Connected LAN



- Each LAN is a ***subnet*** with a "network number."
- Routers identify destination of packets and determine next hop on path
- Router contains separate interface to each of the LANs.
- Interfaces may differ in terms of link layer protocols, physical capabilities and signalling, address spaces, etc.
- Router translates information moving from source LAN to destination LAN.
- To move packets from source to destination, a router will be the next router on the path for the packet. If the destination is on a LAN attached to the router, then the router sends packet to that destination.

Summer Quarter, 2000 C. Irvine; NPS CISR 39

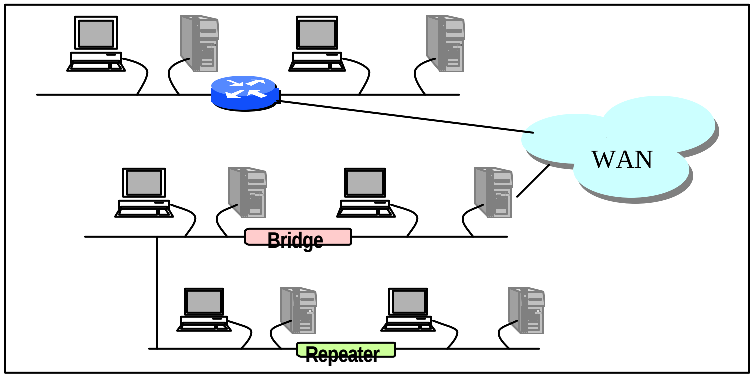
Router Connected LAN Complexity



- Simple and complex LANs can be connected to a router. The router may be connected to a wide area network (WAN). Sometimes servers will provide router functions.

Summer Quarter, 2000 C. Irvine; NPS CISR 40

Enterprise Network



- Enterprise network is built of simple and combined LANS interconnected by routers.

Summer Quarter, 2000 C. Irvine; NPS CISR 41

Internet Naming and Addressing

- Network components are named:
  - carina.cs.nps.navy.mil
  - homunculus.cs.nps.navy.mil
  - even printer has a name:eta.cs.nps.navy.mil
- Each host has a unique IP address.
  - Current IP addresses are 32 bits.
  - A portion identifies subnet and another portion provides a unique host identifier.
- Address assignment is controlled and standardized

Summer Quarter, 2000 C. Irvine; NPS CISR 42

Internet Routing

- Routing moves packets from source to destination hosts. Requirements
  - ★ addresses must be global
    - every host must be able to send packets to every other host
  - ★ Use of address space must be efficient
    - Address space must support efficient routing schemes.
- There are three classes of addresses
  - ★ Class A - for large networks - national networks
  - ★ Class B - for networks likely to have more than 255 hosts
  - ★ Class C - smaller networks
- Each address is composed of four 1-byte octets.

Summer Quarter, 2000 C. Irvine; NPS CISR 43